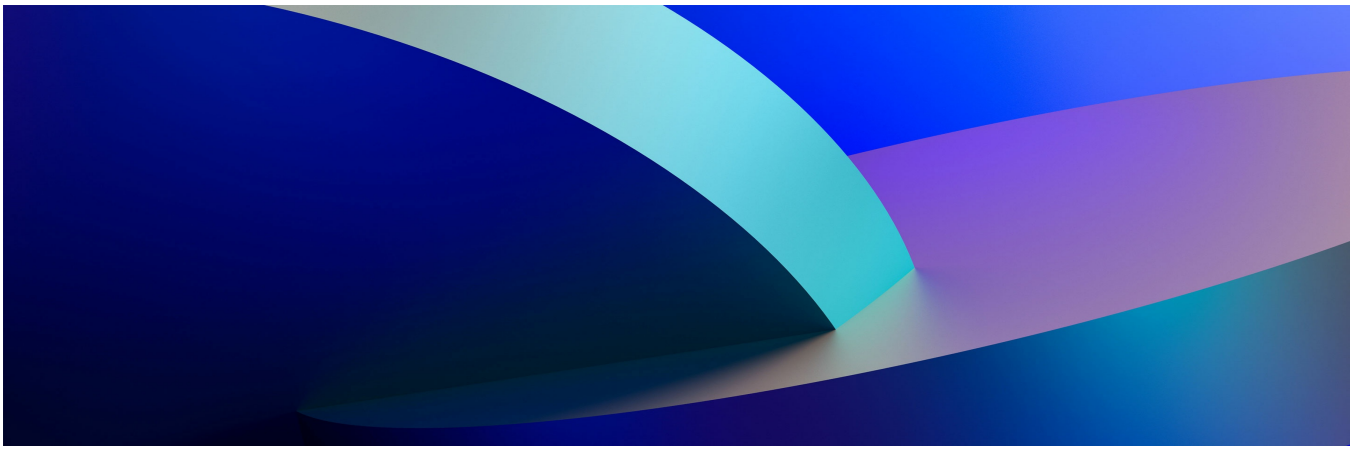

# Data protection and cybersecurity laws in Algeria

## Data protection

### 1. Local data protection laws and scope

The law Nr 18-07 dated on 10 June 2018 related to the protection of private persons in the processing of personal data (hereafter the "Law") has set out the conditions of the collection, recording, organisation, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, reconciliation or interconnection, as well as locking, encryption, erasure or destruction of any information, whatever its support, concerning an identified or identifiable person, directly or indirectly, in particular by reference to an identification number or to one or more elements specific to their physical, physiological, genetic, biometric, psychic, economic, cultural or social identity.

Despite its publication on 2018, the entry in force of this Law is subject to the actual installation of the authority in charge of protection of personal data which is until now (February 2021) not installed yet.

### 2. Data protection authority

The National Authority for the Protection of Personal Data (hereafter the "Authority") is an independent and autonomous authority composed by magistrates, representatives of parliament, senate, human right council, administrations and other persons designated by the President.

It is in charge of receiving declarations and deliver authorisations, put in place rules for the protection of personal data and to settle litigations.

The National Authority for the Protection of Personal Data is not formally established yet.

### 3. Anticipated changes to local laws

Notwithstanding the installation of the Authority, it is expected that executive decrees will be published for the entry into force of the Law.

### 4. Sanctions & non-compliance

There are several types of sanctions for each kind of infringement to the rules related to protection of personal data.

**Administrative sanctions:**

In case of non-respect of the rules related to data protection, the abovementioned authority can decide the following administrative sanctions:

- the warning;
- the notice;
- provisional withdrawal for a period that may not exceed one year, or the definitive withdrawal of the declaration receipt or authorisation;
- an administrative fine up to DZD 500,000 (EUR 3,100).

**Criminal sanctions:**

There are various criminal offences under the law among others:

- unlawful obtaining of personal data;
- misuse of the collected personal data;
- transfer of personal data without authorisation;
- destroying or falsifying information and documents;
- making false statements in response to an information notice or obstruction to the work of the authority; and
- altering personal data to prevent disclosure to the data subject.

Sanctions may vary between two months to five years imprisonment and from DZD 20,000 to DZD 500,000 (EUR 120 to EUR 3,100).

In addition to the organisation, individual company directors can face criminal liability (fines and custodial sentences).

**Others:**

The above-mentioned Authority has the following enforcement powers:

- to impose information notices and publish them;
- to impose the destruction of the data and/or its removal or closing;
- to impose encryption of the data;
- entry and inspection.

A data subject may (in addition to making a complaint to the Authority) also make a claim to the courts for compensation for material or non-material damage (which may include distress).

### 5. Registration / notification / authorisation

There are two kinds of regimes:

- The **declaration**, which is related to data processing that is not likely to infringe the rights and freedoms of the data subjects and their privacy;
- The **authorisation**, when the processing can endanger or may disrespect privacy and freedoms and fundamental rights of individuals.

In case the collected data is used to keep a register, which is accessible to the public or to any person proving a legitimate interest, a simple notification of the identity of the data controller is needed.

### 6. Main obligations and processing requirements

Any personal data processing is subject to a prior declaration to the national Authority or its authorisation.

The controller must implement the appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access, in particular when the processing involves data transmission in a network, as well as against any other form of unlawful processing.

The controller as well as the persons who, in the performance of their duties, have knowledge of personal data, are required to respect professional secrecy even after having ceased to exercise their functions, under criminal sanctions.

Any person acting under the authority of the controller or that of the subcontractor who has access to personal data may only process them on the instruction of the controller, except in the case of execution of a legal obligation.

When the controller is not established on Algerian territory, he or she must notify the national authority of the identity of his or her representative installed in Algeria who, without prejudice to his personal responsibility, replaces him in all his rights and obligations resulting from the provisions of the law.

Interconnection of files containing personal data must obtain prior authorisation of the Authority.

The processing of personal data with a purpose of public interest research, study or evaluation in the field of health is authorised by the national authority, in compliance with

principles defined by this law and according to the public interest that the research, study or evaluation presents.

There is no age limit regarding the data subject. The law has mentioned however that a “child” needs the prior consent of his or her legal guardian or the judge.

Processing of personal data that reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership of the data subject or which relates to his health including his genetic data is forbidden except when:

- the processing is necessary for the safeguard of vital interests of the data subject or of another person and if the data subject is physically or legally unable to give consent;
- the processing is carried out, with the consent of the data subject, by a foundation, association or non-profit organisation of a political, philosophical, religious or trade union nature, within the framework of its legitimate activities, provided that the processing concerns only the members of this body or the persons who maintain regular contact with it related to its purpose that the data are not communicated to third parties without the consent of the persons concerned.
- the processing relates to data clearly made public by the data subject, as long as his or her consent to the processing of the data can be inferred from his or her statements;
- the processing is necessary for the recognition, exercise or defence of legal claims and is carried out exclusively for this purpose;
- the processing of genetic data, excluding those carried out by doctors or biologists and which are necessary for the practice of preventive medicine, medical diagnostics and the administration of care or treatment.
- Personal data relating to offences, penalties and security measures can only be processed by the judicial authority, public authorities, legal persons who manage a public service and court officials within the framework of their legal powers.

**7. Data subject rights**

The data subject must be expressly and unequivocally informed in advance by the person responsible

for the data processing or his or her representative of the following elements :

- the identity of the controller and, where applicable, his or her representative;
- the purposes of the processing;
- the identity of the recipient of the data;
- the information about the transfer of data abroad;
- any additional useful information including the obligation to respond and its consequences as well as the rights of the data subject.

The data subject has an access right to his or her data and is entitled to obtain:

- confirmation of whether his or her personal data is processed or not, the purposes of the processing, the categories of data to which it relates and the recipients;
- communication, in an intelligible form, of his or her data which is the subject of processing, as well as any available information on the origin of the data.

The data subject has the right of rectification and to obtain:

- updating, rectification, erasure or blocking of personal data whose processing does not comply with this law, in particular because of the incomplete or inaccurate nature of such data or whose processing is prohibited by the law. The controller is required to make the necessary corrections at no cost to the requester, within ten days of referral.
- notification to third parties to whom the personal data has been communicated of any updating, rectification, erasure or blocking of personal data carried out in accordance with point above.

The data subject has the objection right, for legitimate reasons, to the processing of his personal data.

He or she has the right to object to use his or her data for prospecting purposes, in particular commercial purposes.

**8. Processing by third parties**

Any third-party subcontractor must provide sufficient guarantees on the technical security and organisational measures relating to the processing to be carried out and must ensure compliance with these measures.

Any subcontracting must be governed by a contract or a legal act (in writing or under another equivalent form) that binds the subcontractor to the controller and which provides in particular that the subcontractor acts only under the sole instruction of the controller and in compliance with the obligations provided for in the law (mainly those related to confidentiality and security of the data).

**9. Transfers out of country**

The controller may transfer personal data to a foreign state with the authorisation of the national authority, only if that state provides a sufficient level of legal protection. It is prohibited, in any case, to communicate or transfer personal data to a foreign country, when such transfer is likely to endanger public security or the vital interests of the State.

It is possible to transfer data abroad when authorised by the data subject, or deemed necessary:

- to safeguard the life of that person;
- to preserve the public interest;
- to comply with obligations to ensure the establishment, exercise or defence of legal claims;
- to perform a contract between the controller and the data subject;
- to conclude or perform a contract concluded or to be concluded, in the interest of the data subject, between the controller and a third party;

- to execute an international legal assistance measure;
- to prevent, diagnose or treat medical conditions.

**10. Data Protection Officer**

Any natural or legal person, public or private or any other entity which, alone or jointly with others, determines the purposes and means of data processing is the designated data controller.

Data controller is responsible to the data subject regarding all the commitments related to the rights of the latter. He or she is also liable towards the Authority regarding general commitments before and during processing of data.

**11. Security**

The data controller must guarantee that any person working for him or her or on his or her behalf, any subcontractor, any representative and any participant in the data processing will respect the general commitments of confidentiality and security of the data notwithstanding the respect of the rights of the data subject.

**12. Breach notification**

The Law has not defined the conditions for introducing a claim, appeal or complaint relating to the implementation of the processing of personal data. The Law specified that the Authority is in charge of informing the plaintiff about the consequences for a breach notification

**13. Direct marketing**

Direct prospecting is forbidden except by email under certain conditions.

**14. Cookies and adtech**

There is no provision related to cookies and adtech in the Law.

**15. Risk scale**

Moderate.

**16. Useful links**

N/A

## Cybersecurity

**1. Local cybersecurity laws and scope**

As regard to the security, please note that there is no particular law related to cybersecurity in Algeria. However, there are general provisions of the regulation in force applicable to different areas, which provide for the concept of the electronic privacy and data protection as well as information security and secrecy, etc. These provisions have a preventive and repressive character in order to fight any criminal acts (e.g. corruption, terrorism, attacks on state security, money laundering and terrorism financing, smuggling, fraudulent use of data, technology and communication offences, discrimination and hate speech, etc).

As an indication, these are some of the provisions:

- The Criminal Code in its Articles 394bis and following protects the right of protection of the integrity of automated data processing systems;
- The Law n° 09-04 of 5 August 2009 on the specific rules relating to the prevention and the fight

against breaches related to technology and communication (Law 09-04);
- The Law No. 18-04 of 10 May 2018 establishing the general rules relating to the post and electronic communications (Law 18-04);
- The Decrees related to licences to operate public telecommunication networks;
- Decision N° 48/SP/PC/ARPT/17 dated 29 November 2017 approving the specifications defining the conditions and modalities for the establishment and operation of hosting and storage services for computerised content for user benefit in the context of cloud computing services (Decision N° 48/SP/PC/ARPT/17);
- The Decree n° 02-156 of 9 May 2002 setting the conditions for interconnection of networks and telecommunications services (Decree 02-156).

**2. Anticipated changes to local laws**

We have no knowledge of the existence of any bills underway that relate to cybersecurity.

**3. Application**

- Criminal law provides for the prohibition of any fraudulent access to any system, or the collection, processing, storage, transfer of personal data for criminal reasons and considers as an offender:
  - anyone who fraudulently introduces data into an automated processing system or fraudulently deletes or modifies the data it contains;
  - anyone who willfully and fraudulently: designs, researches, collects, makes available, disseminates or markets data that is stored, processed or transmitted by a computer system;
  - anyone who holds, reveals, discloses, or makes any use whatsoever of the data obtained by the above mentioned means.

- The Law n° 09-04 provides for the measures and rules for offences related to technology and communication, the obligation for service providers to cooperate with judicial police and authorities for this purpose. The principle of access and its details will be described in the request or order of access. It might be the order to provide readable data or more information such as access to a computer system including its encryption codes.
- The above-mentioned surveillance operations may only be carried out with the written authorisation of the competent judicial authority.It may, in some circumstances, be issued to judicial police officers by the General Attorney at the Court of Algiers, for a period of six months renewable, on the basis of a report indicating the nature of the technical process used and its objectives.In the latter case, the technical devices put in place must focus, exclusively, on the collection and the recording of data relating to the prevention and combating of terrorist acts and attacks on the security of the State.
- The Law 18-04 consecrates the principle of protection of the privacy and personal data of subscribers and users of internet networks, defines among other provisions the “cybersecurity” and measures to implement in this regard, and also provides for the obligations of electronic communications operators.
- The Law 18-04 defines cybersecurity as the set of tools, policies, security concepts, security mechanisms, guidelines, risk management methods, actions, training, good practices, guarantees and technologies that can be used to protect electronic communications against any event that could compromise availability, integrity or confidentiality of data stored, processed or transmitted.The authority in charge of the regulation of electronic communications scrutinises and verifies that electronic communications operators respect their commitments to cybersecurity. It is worth mentioning that there are no more details regarding cybersecurity conditions nor sanction in case of infringement.
- The Decrees related to licences to operate public telecommunication networks provide for some provisions applicable to the contractor holding thd telecom licence on the confidentiality of

information and protection of users and personal information, as well as provisions required for national defence and cooperation with governmental authorities, including the applicable sanctions.

- Decision N° 48/SP/PC/ARPT/17, provides for some rules in connection with data protection and security such as the commitment to:
  - establish infrastructure on the national territory and ensure that this uses equipment integrating the most recent and proven technologies;
  - guarantee that customer data is hosted and stored on national territory;
  - ensure the integrity and confidentiality of customer data except in the cases provided for by the texts in force;
  - guarantee a backup solution for hosted or stored data;
  - establish a customer identification file;
  - do not disclose or use customer data;
  - put in place the necessary mechanisms to ensure the security of data, applications and infrastructure associated with cloud computing, in particular regarding the integrity and confidentiality of data, through the implementation of information security mechanisms against various threats and intrusions;
  - the physical and environmental security of the premises housing the infrastructure, particularly against fires and water damage.
- The Decree n° 02-156 states the obligation for operators and service providers to take all necessary measures to ensure compliance, including: network security; maintenance of network integrity; data protection, including personal, protection of privacy and confidentiality of information processed, transmitted and stored.

### 4. Authority

Regulatory Authority for Post and Electronic Communications: https://www.arpce.dz/fr

### 5. Key obligations

There is no defined process or steps to follow in case of a data breach.

### 6. Sanctions & non-compliance

In case of any infringement the Regulatory Authority for Post and Electronic Communications may decide administrative sanctions. Criminal sanctions fall within the competence of the judge.

#### Administrative sanctions:

Withdrawal of any authorisation.

#### Criminal sanctions:

Sanctions may vary between three months to three years imprisonment, and a fine of DZD 50,000 to DZD 5m (EUR 310 to  EUR 31,000). These penalties are doubled when the offence undermines the national defence of organisations or establishments governed by public rights, without prejudice to the application of more severe penalties. The legal person who has committed the offence is punished by a fine equivalent to five times the maximum of the fine provided for the natural person.

#### Others:

The instruments, programmes and means used in the commission of the offence will be confiscated as well as the closure of sites, subject of one of the offences provided for in this section, and premises and places of operation if the owner is informed.

**7. Is there a national computer emergency response team (CERT) or computer security incident response team (CSIRT)?**

No.

**8. National cybersecurity incident management structure**

There is no such structure.

**9. Other cybersecurity initiatives**

N/A

**10. Useful links**

N/A

# Authors




Amine Sator
left_cms